## CLAIMS

What is claimed is:

1. In an RFID system, a method of communicating securely between a reader and a tag, comprising:

at the reader, modulating an RF carrier signal with a noise encryption signal to produce a noise-encrypted RF carrier signal;

transmitting the noise-encrypted RF carrier signal to the tag; and

at the tag, backscatter modulating the noise-encrypted RF carrier signal with a tag information signal to produce a noise-encrypted backscattered signal.

2. The method of Claim 1, further comprising:

at the reader,

receiving the backscatter modulated noise-encrypted signal;

removing the noise encryption; and

recovering the tag information signal.

3. The method of Claim 1 wherein modulating the RF carrier signal with a noise encryption signal comprises amplitude modulating the RF carrier signal.

4. The method of Claim 1 wherein modulating the RF carrier signal with a noise encryption signal comprises phase modulating or frequency modulating the RF carrier signal.

5. The method of Claim 3 wherein modulating the RF carrier signal with a noise encryption signal further comprises phase modulating or frequency modulating the RF carrier signal.

6. The method of Claim 1 wherein the tag information comprises a tag identification number.

7. The method of Claim 1 wherein the tag information comprises information associated with an item to which the tag is attached.

8. An RFID system, comprising:

a reader operable to modulate an RF carrier signal with a noise encryption waveform and broadcast the resulting noise-encrypted RF carrier signal to a population of tags; and

at least one of the tags of the population of tags configured to receive the noise-encrypted RF carrier signal and backscatter modulate the received noise-encrypted RF carrier signal with a tag information signal.

9. The RFID system of Claim 8 wherein the reader is further operable to receive the backscatter modulated noise-encrypted signal, remove the noise encryption, and recover the tag information signal.

10. The RFID system of Claim 8 wherein the noise encryption waveform includes an amplitude modulation component.

11. The RFID system of Claim 8 wherein the noise encryption waveform includes a phase or frequency modulation component.

12. The RFID system of Claim 11 wherein the noise encryption waveform further includes an amplitude modulation component.

13. The RFID system of Claim 9 wherein the noise encryption waveform includes an amplitude modulation component.

14. The RFID system of Claim 9 wherein the noise encryption waveform includes a phase or frequency modulation component.

15. The RFID system of Claim 14 wherein the noise encryption waveform further includes an amplitude modulation component.

16. A method of preventing an eavesdropper from intercepting a backscattered signal from a tag in an RFID system, comprising:

applying amplitude modulation to a carrier signal generated by a reader;

broadcasting the modulated carrier signal to a tag of the RFID system;

backscatter modulating the modulated carrier signal with tag information.

17. The RFID system of Claim 16, further comprising:

at the reader,

receiving the backscatter modulated signal;

removing the amplitude modulation; and

recovering the tag information.

18. A method of preventing an eavesdropper from intercepting a backscattered signal from a tag in an RFID system, comprising:

applying phase or frequency modulation to a carrier signal generated by a reader;

broadcasting the modulated carrier signal to a tag of the RFID system; and

backscatter modulating the modulated carrier signal with tag information.

19. The method of Claim 18, further comprising:

at the reader,

receiving the backscatter modulated signal;

removing the phase or frequency modulation; and

recovering the tag information.

20. The method of Claim 18, further comprising applying amplitude modulation to the carrier signal, before broadcasting the modulated carrier signal to the tag.

21. The method of Claim 20, further comprising:

at the reader,

receiving the backscatter modulated signal;

removing the amplitude modulation and phase or frequency modulation; and

recovering the tag information.

22. A method of forming an RFID system, comprising:

providing a reader designed to modulate a carrier signal with a noise encryption signal to produce a noise-encrypted carrier signal; and

providing one or more tags designed to receive a broadcast of the noise-encrypted carrier signal and backscatter modulate a reverse link encrypted signal modulated by tag information.

23. The method of Claim 22 wherein the reader is further designed to:

receive the reverse link encrypted signal;

remove the noise encryption; and

recover the tag information.

24. The method of Claim 22 wherein the noise encryption signal comprises an amplitude modulation signal.

25. The method of Claim 22 wherein the noise encryption signal comprises a phase or frequency modulation signal.

26. The method of Claim 25 wherein the encryption signal further comprises an amplitude modulation signal.

27. An RFID system, comprising:

a reader having:

a voltage controlled oscillator (VCO) operable to produce a carrier signal;

a variable gain amplifier (VGA) having a first input configured to receive the carrier signal from the VCO and a second gain control input configured to receive an amplitude modulation signal, said VGA operable to generate an amplitude modulated carrier signal; and

one or more tags configured to receive and backscatter modulate the amplitude modulated carrier signal with tag information stored on the one or more tags,

wherein said amplitude modulation signal operates to noise encrypt the backscatter modulated signal.

28. The RFID system of Claim 27 wherein the VCO includes a phase or frequency control input configured to receive a phase or frequency modulation signal.

29. An RFID system, comprising:

a reader having a voltage controlled oscillator (VCO) configured to receive a phase or frequency modulation signal and provide a phase or frequency modulated carrier signal; and

one or more tags configured to receive and backscatter modulate the phase or frequency modulated carrier signal with tag information stored on the one or more tags,

wherein said phase or frequency modulation signal operates to noise encrypt the backscatter modulated signal.

30. The RFID system of Claim 29 wherein the reader further comprises a variable gain amplifier (VGA) having a first input configured to receive the phase or frequency modulated carrier signal from the VCO and a second gain control input configured to receive an amplitude modulation signal to amplitude modulate the phase or frequency modulated carrier signal, and wherein said amplitude modulation signal operates to further noise encrypt the backscatter modulated signal.

31. A method of establishing a secure two-way communication link between a reader and a tag in an RFID system, comprising:

singulating a tag from a population of tags;

at the reader, modulating a carrier signal with a noise encryption signal;

at the singulated tag, backscatter modulating the noise-encrypted signal with a first portion of a key;

at the reader, verifying that the singulated tag is an authentic tag; and

at the reader, transmitting a second portion of said key to the singulated tag.

32. The method of Claim 31 wherein singulating a tag from a population of tags comprises using information stored on the tag to be singulated, or using a random number generated by the tag to be singulated, in order to prevent exposing tag information prior to completing the establishment of the secure two-way communication link.

33. The method of Claim 32 wherein said information is non-identifying information.

34. The method of Claim 31 wherein the noise encryption signal comprises an amplitude modulation signal.

35. The method of Claim 31 wherein the noise encryption signal comprises a frequency or phase modulation signal.

36. The method of Claim 35 wherein the noise encryption signal further comprises an amplitude modulation signal.

37. The method of Claim 31, further comprising:

at the reader, modifying the value of a portion of the key; and

at the singulated tag, updating the value of the portion of the key according to the modification.

38. The method of Claim 31, further comprising transmitting a password and a lock command from the reader to the singulated tag, so that the singulated tag no longer responds to a reader unless the password is first received by the singulated tag.

39. The method of Claim 31, further comprising transmitting a password and a lock command from the reader to the singulated tag, so that the singulated tag responds to a reader but reveals no information stored on the singulated tag unless the password is first received by the tag.

40. A method of establishing a secure two-way communication link between a reader and a tag in an RFID system, comprising:

singulating a tag from a population of tags;

at the reader, modulating a carrier signal with a noise encryption signal; and

at the singulated tag, backscatter modulating the noise-encrypted signal with a one-time pad.

41. The method of Claim 40 wherein the one-time pad is generated by the tag.

42. The method of Claim 40 wherein the one-time pad is stored on the tag.

43. The method of Claim 40 wherein reader-to-tag communications are encrypted with a function of the one-time pad.

44. The method of Claim 40, further comprising modifying the one-time pad after use.

45. The method of Claim 44 wherein the singulated tag performs the modifying of the one-time pad.

46. The method of Claim 44 wherein the reader requests the modifying of the one-time pad.

47. The method of Claim 44, further comprising:

at the tag, backscatter modulating one or more modified one-time pads; and

at the reader, using said one or more modified one-time pads to secure ongoing communications with the singulated tag.

48. The method of Claim 43, further comprising:

at the singulated tag,

removing the encryption generated by the function of the one-time pad.

49. The method of Claim 40 wherein the noise encryption signal comprises an amplitude modulation signal.

50. The method of Claim 40 wherein the noise encryption signal comprises a frequency or phase modulation signal.

51. The method of Claim 50 wherein the noise encryption signal further comprises an amplitude modulation signal.

52. The method of Claim 40, further comprising transmitting a password and a lock command from the reader to the singulated tag, so that the singulated tag no longer responds to a reader unless the password is first received by the singulated tag.

53. The method of Claim 40, further comprising transmitting a password and a lock command from the reader to the singulated tag, so that the singulated tag responds to a reader but reveals no information stored on the singulated tag unless the password is first received by the tag.

54. A method of establishing a secure two-way communication link between a reader and a tag in an RFID system, comprising:

singulating a tag from a population of tags;

at the reader, modulating a carrier signal with a noise encryption signal;

at the singulated tag, backscatter modulating the noise encrypted signal with a first portion of a key and a one-time pad;

at the reader, verifying that the singulated tag is an authentic tag; and

at the reader, transmitting a second portion of said key to the singulated tag.

55. The method of Claim 54 wherein the second portion of said key is encrypted with a function dependent upon the one-time pad before it transmitted to the singulated key.

56. The method of Claim 54 wherein singulating a tag from a population of tags comprises using information stored on the tag to be singulated, or using a random number generated by the tag to be singulated, in order to prevent exposing tag information prior to completing the establishment of the secure two-way communication link.

57. The method of Claim 56 wherein said information is non-identifying information.

58. The method of Claim 54 wherein the one-time pad is generated by the tag.

59. The method of Claim 54 wherein the one-time pad is stored on the tag.

60. The method of Claim 43 wherein reader-to-tag communications are encrypted with a function of the one-time pad.

61. The method of Claim 54, further comprising modifying the one-time pad after use.

62. The method of Claim 61 wherein the singulated tag performs the modifying of the one-time pad.

63. The method of Claim 61 wherein the reader requests the modifying of the one-time pad.

64. The method of Claim 61, further comprising:

at the tag, backscatter modulating one or more modified one-time pads; and

at the reader, using said one or more modified one-time pads to secure ongoing communications with the singulated tag.

65. The method of Claim 60, further comprising:

at the singulated tag,

removing the encryption generated by the function of the one-time pad.

66. The method of Claim 54 wherein the noise encryption signal comprises an amplitude modulation signal.

67. The method of Claim 54 wherein the noise encryption signal comprises a frequency or phase modulation signal.

68. The method of Claim 67 wherein the noise encryption signal further comprises an amplitude modulation signal.

69. The method of Claim 54, further comprising:

at the reader, modifying the value of a portion of the key; and

at the singulated tag, updating the value of the portion of the key according to the modification.

70. The method of Claim 54, further comprising transmitting a password and a lock command from the reader to the singulated tag, so that the singulated tag no longer responds to a reader unless the password is first received by the singulated tag.

71. The method of Claim 54, further comprising transmitting a password and a lock command from the reader to the singulated tag, so that the singulated tag responds to a reader but reveals no information stored on the singulated tag unless the password is first received by the tag.

72. A reader for an RFID system, comprising:

a noise encryption signal generator; and

a modulator operable to noise encrypt a carrier signal,

wherein said reader is operable to transmit a noise-encrypted RF carrier signal to one or more tags and receive a noise-encrypted backscatter signal modulated by tag information, when the reader is configured in the RFID system.

73. The reader of Claim 72 wherein the noise encryption signal generator includes apparatus configured to generate an amplitude modulation signal.

74. The reader of Claim 72 wherein the noise encryption signal generator includes apparatus configured to generate a phase modulation or frequency modulation signal.

75. The reader of Claim 74 wherein the noise encryption signal generator further includes apparatus configured to generate an amplitude modulation signal.

76. The reader of Claim 72 wherein the reader further includes apparatus configured to remove the noise encryption from the received noise-encrypted backscatter signal and recover the tag information.

77. A reader for an RFID system, comprising:

means for noise encrypting an RF carrier signal broadcast to a tag;

means for receiving a noise-encrypted backscatter modulated signal from the tag;

means for removing the noise encryption from the received noise-encrypted backscatter modulated signal; and

means for recovering tag information sent in the noise-encrypted backscatter modulated signal.

78. The reader of Claim 77 wherein said means for noise encrypting an RF carrier signal comprises means for generating an amplitude modulation signal.

79. The reader of Claim 77 wherein said means for noise encrypting an RF carrier signal comprises means for generating a phase modulation or frequency modulation signal.

80. The reader of Claim 79 wherein said means for noise encrypting an RF carrier signal further comprises means for generating an amplitude modulation signal.